(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－247027
（P2002－247027A）
(43)公開日　平成14年８月30日(2002.8.30)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/18		Ｇ０６Ｆ　7/72		５Ｂ０５６
Ｇ０６Ｆ　7/72			17/10	Ｚ　５Ｊ１０４
17/10		Ｈ０４Ｌ　9/00	６５１	

審査請求　有　　請求項の数６　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－44174(P2001－44174)

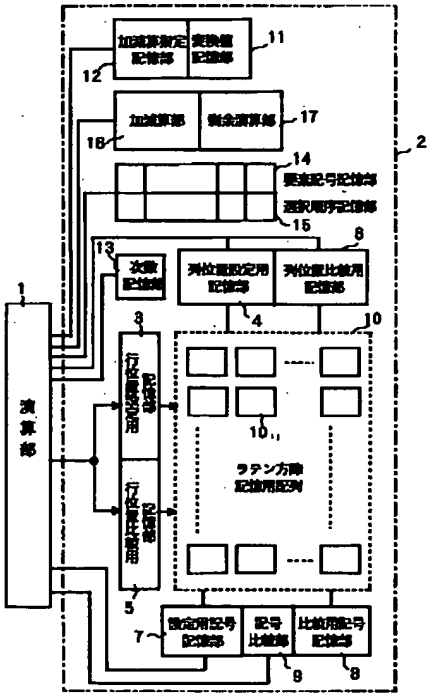
(22)出願日　平成13年２月20日(2001.2.20)

(71)出願人　599161890
エヌイーシーネットワーク・センサ株式会社
東京都府中市日新町一丁目10番地
(72)発明者　伊東　徹
東京都府中市日新町１丁目10番地　エヌイーシーネットワーク・センサ株式会社内
(74)代理人　100085235
弁理士　松浦　兼行

Ｆターム(参考)　5B056 BB00 HH00
5J104 AA01 AA21 JA17 NA17

(54)【発明の名称】　ラテン方陣の作成方法及び作成装置

(57)【要約】
【課題】　記号の配列と選択順に従った配列であるラテン方陣の作成方法では、次に作成されるラテン方陣が一意的に定まるために、暗号などの利用においては、使用するラテン方陣を推測されないとも限らない。
【解決手段】　演算部１は、ラテン方陣記憶用配列１０に設定された既存のｎ次ラテン方陣に記憶された記号を、設定された選択順序で、かつ、選択方向に順次取り込み、取り込んだ記号の値の順番の変換値を、変換値記憶部１１及び加減算指定記憶部１２から読み出し、加減算部１６により変換値を用いて得られた加減算結果に剰余演算部１７でモジュロｎの演算を行わせ剰余結果を得、その剰余結果に応じた記号を、取り込んだ記号の位置の記号ｍとして記憶する変換動作をラテン方陣の最終位置になるまで繰り返す。これにより、ラテン方陣の記憶パターンはそのままであるが、記憶されている要素の配列の選択順を変化させる効果を得る。



1

【特許請求の範囲】

【請求項1】　互いに異なるｎ個の記号ｍを、同じ行と同じ列の各位置ではそれぞれ異なるように、ｎ行ｎ列の位置に配列要素としてそれぞれ設定した次数ｎのラテン方陣を作成する作成方法において、

前記次数ｎと、前記記号ｍの選択順序と、前記ｎ行ｎ列のうちの前記記号ｍが最初に配列される位置と、前記記号ｍを前記ｎ行ｎ列の行方向又は列方向に沿って配列する順序とをそれぞれ設定すると共に所望の既存のｎ次ラテン方陣を記憶用配列に設定し、更に該ｎ次ラテン方陣のｎ個の記号ｍの選択順序或いは記号そのものに各々加算又は減算する整数の変換値を用意する第１のステップと、

前記記憶用配列に設定されている前記既存のｎ次ラテン方陣の設定された位置の記号ｍを取り込み、その記号ｍの選択順序あるいは記号ｍそのものに、前記整数の変換値を加算或いは減算し、その加算又は減算結果を前記ｎで剰余をとった値を選択順序の順番の記号に、該設定された位置の記号ｍとして変換する第２のステップと、

前記第２のステップにより前記記号ｍが変換された位置が、前記ｎ行ｎ列の最終位置であるか否か判定する第３のステップと、

前記第３のステップにより前記最終位置ではないと判定されたときは、前記記号を変換する位置を前記第１のステップにより設定された記号配列方向に従う次の位置を前記設定された位置に指定して、前記第２のステップによる記号の変換を再び行わせ、前記最終位置であると判定されたときは処理を終了する第４のステップとを含むことを特徴とするラテン方陣の作成方法。

【請求項2】　前記第４のステップは、前記第２のステップによるｎ次ラテン方陣のすべての記号の変換を、予め設定した一又は二以上の回数、繰り返したときの最終位置を、前記最終位置と判定して処理を終了することを特徴とする請求項１記載のラテン方陣の作成方法。

【請求項3】　前記第４のステップにより前記最終位置であると判定されたときの前記記憶用配列におけるｎ次ラテン方陣に対して、更に該ｎ次ラテン方陣の各位置の配列要素として記号を順に選択決定するに際して、選択決定を、行及び列の最後の位置から始めて、行又は列に沿って行又は列の最後の位置まで順に行うと共に、各位置毎に同一行、及び同一列の前の位置の既に決定されている配列要素と同一記号とならないように、記号を選択順に選択して、その位置で選択決定することのできる記号が無いときには、その位置より前の位置で既に決定されている配列要素の記号を、該記号よりも順が下位である選択できる記号に代えて選択決定を継続することでラテン方陣を作成する第５のステップを更に含むことを特徴とする請求項１又は２記載のラテン方陣作成方法。

【請求項4】　ｎ行ｎ列の全部でｎ^{2}個の記憶素子を有し、該記憶素子のそれぞれには、互いに異なるｎ個の記号のうち、任意に選択した１つの記号ｍが格納されるラテン方陣記憶用配列と、

前記ラテン方陣記憶用配列を構成するｎ^{2}個の前記記憶素子のうち、設定された位置の記憶素子を指定する指定手段と、

要素の記号の選択順序の値又は要素の記号の値そのものを変化させるための変換値を記憶した変換値記憶部と、

前記変換値の加算又は減算の指定を行う加減算指定部と、

前記記号の選択順序又は前記記号ｍそのものに、前記変換値を加算或いは減算し、その加算又は減算結果を前記ｎで剰余をとる演算を行う剰余計算手段と、

作成しようとするラテン方陣の次数ｎと、前記記号ｍの選択順序と、前記ラテン方陣記憶用配列の前記記号ｍが最初に配列される位置と、前記記号ｍを前記ラテン方陣記憶用配列の行方向又は列方向に沿って配列する順序とをそれぞれ予め設定し、前記指定手段を制御して前記ラテン方陣記憶用配列に設定された既存のｎ次ラテン方陣に記憶された記号を設定された選択順序で、かつ、選択方向に順次取り込み、取り込んだ記号の値の順番の前記変換値を前記変換値記憶部から読み出して、前記剰余計算手段により計算させ、得られた剰余結果の値を選択順序の順番の記号に、該設定された位置の記号ｍとして変換する変換動作を、該記号設置位置が前記ｎ行ｎ列の最終位置になるまで繰り返す演算部とを有し、前記ラテン方陣記憶用配列に設定されている既存のラテン方陣のすべての記号を、前記剰余計算手段により得られた剰余結果の値を用いて変換することにより新たなラテン方陣を作成することを特徴とするラテン方陣作成装置。

【請求項5】　前記演算部は、前記ｎ次ラテン方陣のすべての記号の変換を、予め設定した一又は二以上の回数、繰り返したときの最終位置を、前記最終位置と判定して処理を終了することを特徴とする請求項４記載のラテン方陣の作成装置。

【請求項6】　前記演算部は、前記最終位置であると判定されたときの前記ラテン方陣記憶用配列におけるｎ次ラテン方陣に対して、更に該ｎ次ラテン方陣の各位置の配列要素として記号を順に選択決定するに際して、選択決定を、前記指定手段を制御して行及び列の最後の位置から始めて、行又は列に沿って行又は列の最後の位置まで順に行うと共に、各位置毎に同一行、及び同一列の前の位置の既に決定されている配列要素と同一記号とならないように、記号を選択順に選択して、その位置で選択決定することのできる記号が無いときには、その位置より前の位置で既に決定されている配列要素の記号を、該記号よりも順が下位である選択できる記号に代えて選択決定を継続することでラテン方陣を作成することを特徴とする請求項４又は５記載のラテン方陣の作成装置。

【発明の詳細な説明】

【０００１】

3

【発明の属する技術分野】本発明はラテン方陣の作成方法及び作成装置に係り、特に暗号通信や識別用パスワード作成に使用される変換表とか、実験計画法、統計学における同一性を持たない組み合わせの設定等に利用されるラテン方陣の作成方法及び作成装置に関する。

【0002】

【従来の技術】ラテン方陣の基本的性質は、文献（岩波数学辞典第3版、岩波書店）に詳細に開示されているが、このラテン方陣について簡単に説明する。n個の記号からなる集合A＝{a1，．．．．．an}の各元をn回ずつ使って、合計n^2個をそれぞれn行n列の正方形に配列し、各行各列において、集合Aの各元が1度ずつ現れるものをA上のラテン方陣、あるいはn次ラテン方陣という。

【0003】また、第1行及び第1列が共に自然順列であるものを規約な、あるいは標準形のラテン方陣という。その既約な、あるいは標準形のラテン方陣の個数をL（n）で表すと、n次ラテン方陣の総数はn！・（n－1）！・L（n）となる。L（n）の値はnが9以下のとき、すなわち、n＝1～9のときは次の通りになる。

【0004】L（1）＝1
L（2）＝1
L（3）＝1
L（4）＝4
L（5）＝56
L（6）＝9，408
L（7）＝16，942，080
L（8）＝535，281，401，856
L（9）＝377，597，570，964，258，816

【0005】図8（a）は4次の要素A＝{0，1，2，3}のラテン方陣の基本形を示す。このラテン方陣の基本形は、1行目と1列目の配列要素のいずれもが0～3の昇順（自然順列）になっているので、図8（b）に示す標準形ラテン方陣に属するものとなる。なお、図8（b）において、（・）の配列要素の値は、ラテン方陣を形成する0～3までの任意の値が設定されているものとする。このようなラテン方陣を規則的に作成する方法を、本発明者は先に特開平10－105544号公報にて開示した。

【0006】この発明者の提案になるラテン方陣作成方法では、作成するラテン方陣の次数と記号とを設定し、ラテン方陣の各位置の配列要素として記号を順に選択決定するに際して、行あるいは列に沿って順に選択決定すると共に、各位置毎に同一行及び列の前の位置と同一記号とならないように、記号を選択順に選択してラテン方陣を作成する。

【0007】

【発明が解決しようとする課題】しかるに、上記の本発明者の提案になるラテン方陣作成方法では、作成されるラテン方陣の順序は記号の順列と選択順に従った順であり、この方法では、次に作成されるラテン方陣が一意的に定まるために、暗号などへの利用においては、使用するラテン方陣を推測されないとも限らないという問題がある。

4

【0008】本発明は上記の点に鑑みなされたもので、既存のラテン方陣から所望する同一次数の新たなラテン方陣を一定の手順に従って、特定の変換情報を用いて作成することにより、第三者には既存のラテン方陣と変換情報を知らなければ特定のラテン方陣の作成が困難となるが、作成情報を知っている場合には、正確にラテン方陣を作成し得るラテン方陣作成方法及び作成装置を提供することを目的とする。

【0009】また、本発明の他の目的は、ラテン方陣の利用範囲を広げ、かつ、ラテン方陣の利用価値及び利用効果を飛躍的に高め得るラテン方陣の作成方法及び作成装置を提供することにある。

【0010】

【課題を解決するための手段】本発明は上記の目的を達成するため、第1の発明のラテン方陣の作成方法は、互いに異なるn個の記号mを、同じ行と同じ列の各位置ではそれぞれ異なるように、n行n列の位置に配列要素としてそれぞれ設定した次数nのラテン方陣を作成する作成方法において、次数nと、記号mの選択順序と、n行n列のうちの記号mが最初に配列される位置と、記号mをn行n列の行方向又は列方向に沿って配列する順序とをそれぞれ設定すると共に所望の既存のn次ラテン方陣を記憶用配列に設定し、更にn次ラテン方陣のn個の記号mの選択順序或いは記号そのものに各々加算又は減算する整数の変換値を用意する第1のステップと、記憶用配列に設定されている既存のn次ラテン方陣の設定された位置の記号mを取り込み、その記号mの選択順序あるいは記号mそのものに、整数の変換値を加算或いは減算し、その加算又は減算結果をnで剰余をとった値を選択順序の順番の記号に、設定された位置の記号mとして変換する第2のステップと、第2のステップにより記号mが変換された位置が、n行n列の最終位置であるか否か判定する第3のステップと、第3のステップにより最終位置ではないと判定されたときは、記号を変換する位置を第1のステップにより設定された記号配列方向に従う次の位置を設定された位置に指定して、第2のステップによる記号の変換を再び行わせ、最終位置であると判定されたときは処理を終了する第4のステップとを含むことを特徴とする。

【0011】この発明では、記憶用配列にあらかじめ設定された所望の既存のn次ラテン方陣の各位置の記号を、設定された順番で順次に取り込むと共に、その記憶用配列から取り込んだ記号mに対して記号mの選択順序あるいは記号mそのものに、整数の変換値を加算或いは

5

減算し、その加算又は減算結果をｎで剰余をとった値を、選択順序の順番の記号に、設定された位置の記号ｍとして変換して記憶することを、既存のｎ次ラテン方陣のすべての記号ｍについて行うようにしたため、記憶用配列に変換値をもとに変換されたｎ次ラテン方陣を新たに作成することができる。

【００１２】また、上記の目的を達成するため、第２の発明は、第１の発明の第４のステップを、第２のステップによるｎ次ラテン方陣のすべての記号の変換を、予め設定した一又は二以上の回数、繰り返したときの最終位置を、最終位置と判定して処理を終了することを特徴とする。この発明では、特に複数回繰り返した場合は、既存のｎ次ラテン方陣をより変形することができる。ｎ種類の変換値とそれに対して加算減算の２種類の演算から２ｎ通りの変換情報より、変換値が０で加減算を行った場合において値が変化しない１種類のものを除いて最大ｎ－１種類の変形が可能である。

【００１３】また、上記の目的を達成するため、第３の発明のラテン方陣作成方法は、第１の発明の第４のステップにより最終位置であると判定されたときの記憶用配列におけるｎ次ラテン方陣に対して、更にｎ次ラテン方陣の各位置の配列要素として記号を順に選択決定するに際して、選択決定を、行及び列の最後の位置から始めて、行又は列に沿って行又は列の最後の位置まで順に行うと共に、各位置毎に同一行、及び同一列の前の位置の既に決定されている配列要素と同一記号とならないように、記号を選択順に選択して、その位置で選択決定することのできる記号が無いときには、その位置より前の位置で既に決定されている配列要素の記号を、記号よりも順が下位である選択できる記号に代えて選択決定を継続することでラテン方陣を作成する第５のステップを更に含むことを特徴とする。

【００１４】この第３の発明では、記憶用配列に変換情報により変換されたラテン方陣を基にして、更に別のラテン方陣作成方法を組み合わせて別の新たなラテン方陣を作成することができる。上記の別のラテン方陣作成方法は、この第３の発明では、特開平１０－１０５５４４号公報記載のラテン方陣の作成方法である。

【００１５】また、上記の目的を達成するため、第４の発明のラテン方陣作成装置は、ｎ行ｎ列の全部でn^2個の記憶素子を有し、記憶素子のそれぞれには、互いに異なるｎ個の記号のうち、任意に選択した１つの記号ｍが格納されるラテン方陣記憶用配列と、ラテン方陣記憶用配列を構成するn^2個の記憶素子のうち、設定された位置の記憶素子を指定する指定手段と、要素の記号の選択順序の値又は要素の記号の値そのものを変化させるための変換値を記憶した変換値記憶部と、変換値の加算又は減算の指定を行う加減算指定部と、記号の選択順序又は記号ｍそのものに、変換値を加算或いは減算し、その加算又は減算結果をｎで剰余をとる演算を行う剰余計算手段と、作成しようとするラテン方陣の次数ｎと、記号ｍの選択順序と、ラテン方陣記憶用配列の記号ｍが最初に配列される位置と、記号ｍをラテン方陣記憶用配列の行方向又は列方向に沿って配列する順序とをそれぞれ予め設定し、指定手段を制御してラテン方陣記憶用配列に設定された既存のｎ次ラテン方陣に記憶された記号を設定された選択順序で、かつ、選択方向に順次取り込み、取り込んだ記号の値の順番の変換値を変換値記憶部から読み出して、剰余計算手段により計算させ、得られた剰余結果の値を選択順序の順番の記号に、設定された位置の記号ｍとして変換する変換動作を、記号設置位置がｎ行ｎ列の最終位置になるまで繰り返す演算部とを有し、ラテン方陣記憶用配列に設定されている既存のラテン方陣のすべての記号を、剰余計算手段により得られた剰余結果の値を用いて変換することにより新たなラテン方陣を作成する構成としたものである。

【００１６】この第４の発明では、ラテン方陣記憶用配列に設定されている既存のラテン方陣のすべての記号を、変換値記憶部に記憶されている変換値を用いて変換することにより新たなラテン方陣を作成することを特徴とする。

【００１７】また、上記の目的を達成するため、第５の発明は、第４の発明の演算部を、ｎ次ラテン方陣のすべての記号の変換を、予め設定した一又は二以上の回数、繰り返したときの最終位置を、最終位置と判定して処理を終了することを特徴とする。

【００１８】更に、上記の目的を達成するため、第６の発明は、演算部を、最終位置であると判定されたときのラテン方陣記憶用配列におけるｎ次ラテン方陣に対して、更にｎ次ラテン方陣の各位置の配列要素として記号を順に選択決定するに際して、選択決定を、指定手段を制御して行及び列の最後の位置から始めて、行又は列に沿って行又は列の最後の位置まで順に行うと共に、各位置毎に同一行、及び同一列の前の位置の既に決定されている配列要素と同一記号とならないように、記号を選択順に選択して、その位置で選択決定することのできる記号が無いときには、その位置より前の位置で既に決定されている配列要素の記号を、記号よりも順が下位である選択できる記号に代えて選択決定を継続することでラテン方陣を作成することを特徴とする。この第６の発明では、変換値を用いて変換してラテン方陣を新たに作成した後、更に別のラテン方陣作成方法でラテン方陣を作成するようにしたため、ラテン方陣要素の変化が不規則にできる。

【００１９】

【発明の実施の形態】次に、本発明の一実施の形態について図面と共に説明する。なお、以下の説明では、説明の便宜上、次数ｎを４とし、記号ｍは自然数の要素Ａ＝｛０，１，２，３｝とし、その順列及び選択順は自然順列の通り（０，１，２，３）とする。

【００２０】図１は本発明になるラテン方陣の作成装置の一実施の形態のブロック図を示す。同図において、演算部１は、ソフトウェア的に演算処理を実行する他に、次数ｎと、記号ｍの選択順序と、ｎ次ラテン方陣のｎ行ｎ列のうちの記号ｍが最初に配列される位置と、記号ｍをｎ行ｎ列の行方向又は列方向に沿って配列する順序とをそれぞれ設定すると共に、既存のラテン方陣のラテン方陣記憶用配列１０への設定を行う回路部で、この演算部１は予め定められた制御プログラムに従って各種の演算の実行を行い、接続されているラテン方陣作成部２において作成するラテン方陣Ｒのデータの行列位置の指定と比較判断及び設定、読み取りを行う。

【００２１】ラテン方陣作成部２は、演算部１に接続されており、行位置設定用記憶部３、列位置設定用記憶部４、行位置比較用記憶部５、列位置比較用記憶部６、設定用記号記憶部７、比較用記号記憶部８、記号比較部９、ラテン方陣記憶用配列１０、変換値記憶部１１、加減算指定記憶部１２、次数記憶部１３、要素記号記憶部１４、選択順序記憶部１５、加減算部１６及び剰余演算部１７から構成されている。

【００２２】行位置設定用記憶部３は、演算部１の出力信号に基づいて選択決定される記号ｍの行位置を、ラテン方陣記憶用配列１０に対して指定する。列位置設定用記憶部４は、演算部１の出力信号に基づいて選択決定される記号ｍの列位置を、ラテン方陣記憶用配列１０に対して指定する。

【００２３】行位置比較用記憶部５は、演算部１の出力信号に基づいて選択決定される記号ｍと比較される記号ｍ’の行位置を、また、列位置比較用記憶部６は、演算部１の出力信号に基づいて選択決定される記号ｍと比較される記号ｍ’の列位置を、それぞれラテン方陣記憶用配列１０に対して指定する。また、設定用記号記憶部７は、演算部１の出力信号に基づいて選択決定される記号ｍを記憶したり、ラテン方陣記憶用配列１０からの記号ｍを記憶する。

【００２４】比較用記号記憶部８は、ラテン方陣記憶用配列１０から読み出された、比較される記号ｍ’を記憶する。記号比較部９は、設定用記号記憶部７に記憶された、演算部１により設定されたデータｍと、比較用記号記憶部８に記憶された、比較される記号ｍ’とを比較し、その比較結果を演算部１へ出力する。ラテン方陣記憶用配列１０には、予め既存のｎ次ラテン方陣が作成されている。

【００２５】変換値記憶部１１は変換値の絶対値を記憶し、加減算指定記憶部１２でラテン方陣の要素の値、或いは要素の選択順序の値に、変換値の符号に応じて加算あるいは減算するための指定を行う。次数記憶部１３は、作成を行うラテン方陣の次数ｎの値を記憶し、剰余演算などの各種演算に利用する。要素記号記憶部１４は、作成するラテン方陣に設定される要素記号の値を記憶し、その要素記号に対応する選択順序の順番の値を選択順序記憶部１５に記憶する。

【００２６】加減算部１６は、ラテン方陣の要素の値或いは選択順序の順番の値と変換値に対して加減算指定記憶部１２の指定により、加算あるいは減算を行う。剰余演算部１７は、変換値或いは加減算部１６の演算結果の値を次数記憶部１３に記憶されているラテン方陣の次数ｎの値で剰余、即ちｍｏｄ　ｎ（モデュロｎ）演算を行う。

【００２７】また、ラテン方陣作成部２が作成するラテン方陣Ｒは、次数がｎの場合は図２に示すように、ｎ行ｎ列からなり、Ｉ行Ｊ列の位置はK_{IJ}で表され、その位置K_{IJ}に配列される配列要素（記号ｍ）はE_{IJ}で表される。図１中のラテン方陣記憶用配列１０は、ｎ次のラテン方陣を作成するときには、図２に示したラテン方陣Ｒと同様にｎ行ｎ列の、全部でn^2個の配列子（記憶素子）からなり、そのうちのＩ行Ｊ列の位置K_{IJ}の配列子は10_{IJ}で表される。ここで、各配列子10_{IJ}は、それぞれ１つの記号（データ）ｍを記憶する。

【００２８】演算部１は、作成しようとするラテン方陣の次数ｎと、記号ｍの選択順序と、ラテン方陣記憶用配列１０の記号ｍが最初に配列される位置と、記号ｍをラテン方陣記憶用配列１０の行方向又は列方向に沿って配列する順序とがそれぞれ予め設定され、行位置設定用記憶部３に行位置を、列位置設定用記憶部４に列位置をそれぞれ設定してラテン方陣記憶用配列１０に設定された既存のｎ次ラテン方陣に記憶された記号を、設定された選択順序で、かつ、選択方向に順次取り込み、取り込んだ記号の値の順番の変換値Ｆを、変換値記憶部１１及び加減算指定記憶部１２から読み出し、取り込んだ記号の位置に変換値Ｆで変換した結果を記憶する変換動作をラテン方陣の最終位置になるまで繰り返すことにより、ラテン方陣記憶用配列１０に新たなラテン方陣を作成する。

【００２９】例えば、変換値Ｆを「－３」とし、ラテン方陣記憶用配列１０に設定された既存のｎ次ラテン方陣を図４（ａ）及び図７（ａ）に示す４次のラテン方陣とし、要素記号の値を直接変換するものとすると、変換値Ｆの符号は負であるので減算を指定し、変換値の絶対値「３」でラテン方陣に設定された記号Ａ＝｛０，１，２，３｝を変換することを示す。

【００３０】従って、変換値Ｆが「－３」のときには、ラテン方陣の設定要素「０」に対しては、その値に「３」を減算して－３（＝０－３）の減算結果を得、その減算結果に次数である４（＝ｎ）で剰余をとる（モジュロ４の計算をする）ことにより、要素記号の値は「１」に変換される。設定要素が「１」の時には、変換値との減算結果が－２（＝１－３）であるので、その減算結果に４で剰余をとることにより、要素記号の値は「２」に変換される。同様に、設定要素が「２」の時に

は減算結果は－１（＝２－３）で、減算結果に４の剰余をとることにより、要素記号の値は「３」に変換される。要素記号が「３」の時には、減算結果は０（＝３－３）であるから、減算結果に４の剰余をとることにより、要素記号の値は「０」となる。これにより、すべての要素が新たな要素に変換される。結果の要素の選択順序は（１，２，３，０）となる。

【００３１】なお、変換値の絶対値は、通常は次数ｎより小なる値であるが、加減算を行う変換値の絶対値がｎ以上の場合には、絶対値にｍｏｄ　ｎの演算を行ってｎより小さな値にして加減算を行い、更にｍｏｄ　ｎをして変換結果とするか、変換値要素の値に加減算を行った後でｍｏｄ　ｎを行うことでその結果とすることができる。

【００３２】次に、上記のラテン方陣作成装置を用いて作成される本発明のラテン方陣作成方法について説明する。図３は本発明になるラテン方陣の作成方法の一実施の形態を説明するフローチャートを示す。ここで、演算部１は、図１に示したラテン方陣記憶用配列１０に既存のラテン方陣Ｒ’を行Ｉと列Ｊの各位置$K_{I\ J}$に配置した記号ｍを配列要素$E_{I\ J}$として設定すると共に、演算部１には作成情報として次数ｎと、ｎ行ｎ列のうちの記号ｍが最初に配列される位置と、記号ｍをｎ行ｎ列の行方向又は列方向に沿って配列する順序と、記号ｍの選択順序とがそれぞれ設定されている。更に、変換値記憶部１１に変換値Ｆの絶対値が、加減算指定記憶部１２には変換値Ｆの符号に応じた加算又は減算を設定する。

【００３３】ここでは、一例として、ラテン方陣記憶用配列１０に既存のラテン方陣Ｒ’として、図４（ａ）及び図７（ａ）に示す４次のラテン方陣が予め記憶されており、また、前述したように、次数ｎを４とし、記号ｍは自然数（０，１，２，３）とし、その順列及び選択順は自然順列の通りとする。位置の進行方向は図６（ａ）に矢印で示す方向に進行する列方向と、同図（ｂ）に矢印で示す方向に進行する行方向とがある。ここでは、位置の進行方向は、列方向が設定されたものとする。また、最初の位置は、一般形ラテン方陣では１行１列目の$K_{1\ 1}$である。更に、変換値記憶部１１には「３」が記憶され、加減算指定記憶部１２には減算が指定されている（すなわち、変換値Ｆは「－３」である）ものとする。

【００３４】この状態で、演算部１は、まず、行位置設定用記憶部３に行位置Ｉとして”１”を設定し（ステップＳ１）、続いて、列位置設定用記憶部４に列位置Ｊとして”１”を設定する（ステップＳ２）。これにより、行位置設定用記憶部３と列位置設定用記憶部４により設定されたラテン方陣記憶用配列１０の最初の位置$K_{1\ 1}$の要素Ｅ（１，１）（＝０）が設定用記号記憶部７に出力されて記憶される。

【００３５】続いて、演算部１は設定用記号記憶部７からラテン方陣記憶用配列１０の最初の位置$K_{1\ 1}$の要素Ｅ（１，１）（＝０）を取り込み、それを変換値記憶部１１及び加減算指定記憶部１２から変換値「－３」を読み出して、加減算部１６により要素「０」と変換値の絶対値「３」との減算動作を行わせ、得られた減算結果－３（＝０－３）を、更に剰余演算部１７でモジュロ４の演算を行わせ、１（＝－３　ｍｏｄ　４）の剰余結果を得る。

【００３６】演算部１は、剰余演算部１７で得られた剰余結果「１」を要素の記号として変換し、変換した記号「１」を設定用記号記憶部７から再度、行位置設定用記憶部３及び列位置設定用記憶部４に設定されている位置$K_{1\ 1}$の要素Ｅ（１，１）としてラテン方陣記憶用配列１０の最初の位置$K_{1\ 1}$の要素Ｅ（１，１）に設定する（ステップＳ３）。これにより、ラテン方陣記憶用配列１０は、図４（ｂ）にアンダーラインを付して示すように要素Ｅ（１，１）の記号が「１」に変換される。

【００３７】次に、演算部１は列位置設定記憶部４に設定されている列位置Ｊの値が、次数ｎより小さいかどうか判定する（ステップＳ４）。この時点ではＪ＝１、ｎ＝４であるので、Ｊ＜ｎであるから、列位置Ｊの値を”１”加算して列位置設定用記憶部４に「２」を設定した後（ステップＳ５）、ステップＳ３に進む。この時点では、行位置設定用記憶部３の値は前回と同じ「１」のままである。

【００３８】従って、ステップＳ３では、演算部１は設定用記号記憶部７を通してラテン方陣記憶用配列１０の次の位置$K_{1\ 2}$の要素Ｅ（１，２）（＝１）を取り込み、また、変換値記憶部１１及び加減算指定記憶部１２から読み出した変換情報Ｆの値「－３」に基づき、加減算部１６により要素「１」と変換値の絶対値「３」との減算動作を行わせ、得られた減算結果－２（＝１－３）を、更に剰余演算部１７でモジュロ４の演算を行わせ、２（＝－２　ｍｏｄ　４）の剰余結果を得る。

【００３９】演算部１は、剰余演算部１７で得られた剰余結果「２」を要素の記号として変換し、変換した記号「２」を設定用記号記憶部７から再度、行位置設定用記憶部３及び列位置設定用記憶部４に設定されている位置$K_{1\ 2}$の要素Ｅ（１，２）としてラテン方陣記憶用配列１０の位置$K_{1\ 2}$の要素Ｅ（１，２）に設定する。これにより、ラテン方陣記憶用配列１０は、図４（ｃ）にアンダーラインを付して示すように要素Ｅ（１，２）の記号が「２」に変換される。

【００４０】続いて、演算部１は今度はラテン方陣記憶用配列１０の次の位置$K_{1\ 3}$の要素Ｅ（１，３）（＝２）を取り込み、変換値記憶部１１及び加減算指定記憶部１２から読み出した変換情報Ｆの値「－３」に基づき、加減算部１６により要素「２」と変換値の絶対値「３」との減算動作を行わせ、得られた減算結果－１（＝２－３）を、更に剰余演算部１７でモジュロ４の演

算を行わせ、3（＝－1　mod　4）の剰余結果を得て、それを位置K_{13}の要素E（1，3）としてラテン方陣記憶用配列10に設定する（ステップS4、S5、S3）。これにより、ラテン方陣記憶用配列10の要素E（1，3）は、図4（d）にアンダーラインを付して示すように記号「3」に変換される。

【0041】続いて、演算部1は今度はラテン方陣記憶用配列10の次の位置K_{14}の要素E（1，4）（＝3）を取り込み、変換値記憶部11及び加減算指定憶部12から読み出した変換情報Fの値「－3」に基づき、加減算部16により要素「3」と変換値の絶対値「3」との減算動作を行わせ、得られた減算結果0（＝3－3）を、更に剰余演算部17でモジュロ4の演算を行わせ、0（＝0　mod　4）の剰余結果を得て、それを位置K_{14}の要素E（1，4）としてラテン方陣記憶用配列10に設定する（ステップS4、S5、S3）。これにより、ラテン方陣記憶用配列10の要素E（1，4）は、図4（e）にアンダーラインを付して示すように記号「0」に変換される。

【0042】この段階で、J＝4となり、nの値と等しくなるので、ステップS4を経由して演算部1は行位置設定記憶部3に設定されている行位置Iの値が、次数nより小さいかどうか判定する（ステップS6）。この時点ではI＝1、n＝4であるので、I＜nであるから、行位置Iの値を”1”加算して行位置設定用記憶部3に「2」を設定した後（ステップS7）、ステップS2に進み、列位置設定用記憶部4に設定されている列位置Jの値が「1」に設定される。

【0043】続いて、演算部1はラテン方陣記憶用配列10の次の位置K_{21}の要素E（2，1）（＝1）を取り込み、変換値記憶部11及び加減算指定憶部12から読み出した変換情報Fの値「－3」に基づき、加減算部16により要素「1」と変換値の絶対値「3」との減算動作を行わせ、得られた減算結果－2（＝1－3）を、更に剰余演算部17でモジュロ4の演算を行わせ、2（＝－2　mod　4）の剰余結果を得て、それを位置K_{21}の要素E（2，1）としてラテン方陣記憶用配列10に設定する（ステップS3）。これにより、ラテン方陣記憶用配列10の要素E（2，1）は、図4（f）にアンダーラインを付して示すように記号「2」に変換される。

【0044】以下、上記と同様の動作が繰り返され、演算部1はラテン方陣記憶用配列10の位置K_{43}の要素E（4，3）として、図4（g）にアンダーラインを付して示すように記号「2」に変換し、ラテン方陣記憶用配列10の最後の位置K_{44}の要素E（4，4）として、図4（h）にアンダーラインを付して示すように記号「1」に変換する。この時点ですべての要素の記号が変換されて、J＝4、I＝4となるので、ステップS4及びステップS6をそれぞれ経由してラテン方陣の作成処理を終了する（ステップS8）。

【0045】次に、別の例について図1、図3及び図5と共に説明する。この別の例では、ラテン方陣記憶用配列10に既存のラテン方陣R’として、図5（a）及び図7（c）に示す4次のラテン方陣が予め記憶されており、また、前述したように、次数nを4とし、記号mは（a，b，c，d）とする。位置の進行方向は図6（a）に示す、列方向が設定されたものとする。また、最初の位置は、一般形ラテン方陣では1行1列目のK_{11}である。更に、変換値記憶部11には「2」が記憶され、加減算指定記憶部12には加算が指定されている（すなわち、変換値Fは「＋2」である）ものとする。

【0046】この状態で、演算部1は、まず、行位置設定用記憶部3に行位置Iとして”1”を設定し（ステップS1）、続いて、列位置設定用記憶部4に列位置Jとして”1”を設定する（ステップS2）。これにより、行位置設定用記憶部3と列位置設定用記憶部4により設定されたラテン方陣記憶用配列10の最初の位置K_{11}の要素E（1，1）（＝a）が設定用記号記憶部7に出力されて記憶される。

【0047】続いて、演算部1は設定用記号記憶部7からラテン方陣記憶用配列10の最初の位置K_{11}の要素E（1，1）（＝a）を取り込み、それを変換値記憶部11及び加減算指定記憶部12から変換値「＋2」を読み出して加減算部16に供給する。ここで、ラテン方陣に設定された要素の記号A＝{a，b，c，d}の選択順序を（0，1，2，3）とすると、記号aの選択順序は0であり、加減算部16は、記号aの選択順序「0」と変換値「2」を加算する。

【0048】剰余演算部17は、加減算部16により得られた加算結果2（＝0＋2）で4の剰余をとる（モジュロ4の演算をする）ことで、剰余結果「2」を得る。演算部1はその剰余結果「2」に基づき、選択順序2の記号cを要素の記号として変換し、変換した記号「c」を設定用記号記憶部7から再度、行位置設定用記憶部3及び列位置設定用記憶部4に設定されている位置K_{11}の要素E（1，1）としてラテン方陣記憶用配列10の最初の位置K_{11}の要素E（1，1）に設定する（ステップS3）。これにより、ラテン方陣記憶用配列10は、図5（b）にアンダーラインを付して示すように要素E（1，1）の記号が「c」に変換される。

【0049】続いて、演算部1は今度はラテン方陣記憶用配列10の次の位置K_{12}の要素E（1，2）（＝b）を取り込み、変換値記憶部11及び加減算指定記憶部12から読み出した変換情報Fの値「＋2」に基づき、加減算部16により要素「b」の選択順序である「1」と変換値の絶対値「2」との加算動作を行わせ、得られた加算結果3（＝1＋2）を、更に剰余演算部17でモジュロ4の演算を行わせ、3（＝3　mod　4）の剰余結果を得て、選択順序「3」の記号dに変換

し、それを位置K_{12}の要素E（1，2）としてラテン方陣記憶用配列10に設定する（ステップS4、S5、S3）。これにより、ラテン方陣記憶用配列10の要素E（1，2）は、図5（c）にアンダーラインを付して示すように記号「d」に変換される。

【0050】続いて、演算部1は今度はラテン方陣記憶用配列10の次の位置K_{13}の要素E（1，3）（＝c）を取り込み、変換値記憶部11及び加減算指定記憶部12から読み出した変換情報Fの値「＋2」に基づき、加減算部16により要素「c」の選択順序である「2」と変換値の絶対値「2」との加算動作を行わせ、得られた加算結果4（＝2＋2）を、更に剰余演算部17でモジュロ4の演算を行わせ、0（＝4　mod　4）の剰余結果を得て、選択順序「0」の記号aに変換し、それを位置K_{13}の要素E（1，3）としてラテン方陣記憶用配列10に設定する（ステップS4、S5、S3）。これにより、ラテン方陣記憶用配列10の要素E（1，3）は、図5（d）にアンダーラインを付して示すように記号「a」に変換される。

【0051】続いて、演算部1は今度はラテン方陣記憶用配列10の次の位置K_{14}の要素E（1，4）（＝d）を取り込み、変換値記憶部11及び加減算指定憶部12から読み出した変換情報Fの値「＋2」に基づき、加減算部16により要素「d」の選択順序「3」と変換値の絶対値「2」との加算動作を行わせ、得られた加算結果5（＝3＋2）を、更に剰余演算部17でモジュロ4の演算を行わせ、1（＝5　mod　4）の剰余結果を得て、選択順序「1」の記号bを位置K_{14}の要素E（1，4）としてラテン方陣記憶用配列10に設定する（ステップS4、S5、S3）。これにより、ラテン方陣記憶用配列10の要素E（1，4）は、図5（e）にアンダーラインを付して示すように記号「b」に変換される。

【0052】この段階で、J＝4となり、nの値と等しくなるので、ステップS4を経由して演算部1は行位置設定記憶部3に設定されている行位置Iの値が、次数nより小さいかどうか判定する（ステップS6）。この時点ではI＝1、n＝4であるので、I＜nであるから、行位置Iの値を”1”加算して行位置設定用記憶部3に「2」を設定した後（ステップS7）、ステップS2に進み、列位置設定用記憶部4に設定されている列位置Jの値が「1」に設定される。

【0053】以下、上記と同様の動作が繰り返され、ラテン方陣記憶用配列10の要素E（2，1）は、図5（f）にアンダーラインを付して示すように記号「d」に、要素E（4，3）は、図5（g）にアンダーラインを付して示すように記号「d」に、要素E（4，4）は、図5（h）にアンダーラインを付して示すように記号「c」にそれぞれ変換される。この時点ですべての要素の記号が変換されて、J＝4、I＝4となるので、ステップS4及びステップS6をそれぞれ経由してラテン方陣の作成処理を終了する（ステップS8）。この実施の形態では、結果の要素の選択順序は（c，d，a，b）となる。

【0054】このように、本実施の形態によれば、既存のラテン方陣のそれぞれの要素を、変換値記憶部11に記憶されている変換値Fによって要素を変換することによって、ラテン方陣の記憶パターンはそのままであるが、記憶されている要素の配列の選択順を変化させたのと同じ効果が得られ、既存のラテン方陣と、同一次数のラテン方陣を確実、かつ、簡単に変換させることができる。要素の変換によって、元のラテン方陣をn－1種類の変形が可能となり、利用価値もn－1倍となり、これにより、新たに作成されるラテン方陣の第三者による推測を困難にできる。

【0055】なお、本発明は上記の実施の形態に限定されるものではなく、例えば上記の変換を予め設定した複数回数繰り返して、新たなラテン方陣Rを作成するようにしてもよい。また、本発明者が先に特開平10－10５５４４号公報にて提案したラテン方陣作成方法とを組み合わせて新たなラテン方陣を作成することもできる。上記の本発明者の提案になるラテン方陣作成方法では、作成するラテン方陣の次数nと記号mとを設定し、ラテン方陣Rの各位置の配列要素として記号を順に選択決定するに際して、選択決定を、行及び列の最後の位置から始めて、行又は列に沿って行又は列の最後の位置まで順に行うと共に、各位置毎に同一行、及び列の前の位置の既に決定されている配列要素と同一記号とならないように、記号を選択順に選択して、もし、その位置で選択決定することのできる記号が無いときには、その位置より前の位置で既に決定されている配列要素の記号を、該記号よりも順が下位である選択できる記号に代えて選択決定を継続することでラテン方陣を作成する方法である。

【0056】あるいは、本発明者が先に特願2000－３１０５号で提案したラテン方陣作成方法で作成したラテン方陣とを組み合わせて、新たなラテン方陣を得ることもできる。この提案のラテン方陣作成方法は、互いに異なるn個の記号を、同じ行と同じ列の各位置ではそれぞれ異なるように、n行n列の位置に配列要素としてそれぞれ設定した次数nのラテン方陣を作成する作成方法において、前記次数nと、前記記号mの選択順序と、前記n行n列のうちの前記記号mが最初に配列される位置と、前記記号mを前記n行n列の行方向又は列方向に沿って配列する順序とをそれぞれ設定する第1のステップと、所望の既存のn次ラテン方陣を記憶用配列に設定する第2のステップと、前記既存のn次ラテン方陣の、前記第1のステップで設定された最初の位置の記号の次の選択順の記号を設定し、設定する当該次の選択順の記号が存在しないときは位置を一つ前に戻して、その位置の記号の次の選択順の記号を設定する第3のステップと、

前のステップで設定された記号を、その記号の設定位置と同じ行と同じ列の前の位置の記号とを比較して、同じ記号があるときは前記第3のステップの処理を再度実行させ、同じ記号がないときは前記前のステップで設定された記号を前記記憶用配列に記憶する第4のステップと、前記第4のステップにより記憶された記号の位置が、作成しようとするラテン方陣の最後の位置であるときはすべての処理を終了し、該最後の位置でないときは、指定位置を次の位置に進めて、その位置に選択順の最初の記号を設定してから前記第4のステップの処理を実行させる第5のステップとを含むことを特徴とする。

【0057】これらの本発明者の先の提案になるラテン方陣作成方法により作成したラテン方陣を、上記の実施の形態における既存のラテン方陣R'として用い、上記の実施の形態により作成した新たなラテン方陣を中間ラテン方陣R"とし、この中間ラテン方陣R"を既存のラテン方陣として、更に上記の実施の形態により新たなラテン方陣を作成するか、本発明者の先の提案になるラテン方陣作成方法により作成したラテン方陣を作成するようにしてもよい。すなわち、本発明者の先の提案になるラテン方陣作成方法と上記の実施の形態のラテン方陣作成方法とを組み合わせて1回又は複数回繰り返すことにより、新たなラテン方陣Rを作成するようにしてもよい。

【0058】また、図6（b）に示したように行方向にラテン方陣の各配列要素E[I][J]を作成することができることは勿論であり、また、4次以外の次数のラテン方陣も同様にして作成することができるものである。また、設定される記号mは特に限定されるものではなく、図4（a）や図7（a）に示すように（0，1，2，3）のように0から始まる数値の他に、例えば図7（b）のように（1，2，3，4）のような1から始まる数値とか、図7（c）のように（a，b，c，d）のような順番のアルファベットを任意に設定できる。更には、数値やアルファベット以外に特定の順序の単語その他文字列などにも適用できる。

【0059】同様に、変換値記憶部11は、加減算指定記憶部12と整数値の変換値記憶部11に限らず、正の整数或いは負の整数を加算するという構成でもよく、変換値の絶対値はnより小さな数に限らずnと等しいかそれ以上の数でもよく、更に変換の前にnの剰余をとることも可能である。

【0060】また、変換対象のn次のラテン方陣の要素の記号が0からn－1の場合には、要素に直接変換値を作用することができるが、要素が1からnの場合や文字から構成されている場合には、図5と共に説明したように、要素の記号の選択順序を0からn－1として、その選択順序に変換値を作用して変換された選択順序の記号を設定することで新たなラテン方陣の作成が可能となる。

【0061】

【発明の効果】以上説明したように、第1及び第4の発明によれば、記号mの選択順序あるいは記号mそのものに、整数の変換値を加算或いは減算し、その加算又は減算結果をnで剰余をとった値を、選択順序の順番の記号に、設定された位置の記号mとして変換して記憶することを、既存のn次ラテン方陣のすべての記号mについて行うことにより、記憶用配列に変換値をもとに変換されたn次ラテン方陣を新たに作成するようにしたため、既存のラテン方陣と同一次数のラテン方陣を確実、かつ、簡単に作成することができる。

【0062】また、第2及び第5の発明によれば、変換値をもとに変換されたn次ラテン方陣の作成を複数回繰り返すことにより、最大n－1種類の変形が可能となり、利用価値もn－1倍となり、これにより新たに作成されるラテン方陣の第三者による推測をより一層困難にすることができる。

【0063】更に、第3及び第6の発明によれば、変換値をもとに変換してラテン方陣を新たに作成した後、更に別のラテン方陣作成方法でラテン方陣を作成するようにしたため、ラテン方陣要素の変化が不規則となり、要素の変化の効果も拡大し、これらの作成情報を知らない第三者には、既存のラテン方陣から新たなラテン方陣の推測は困難であるが、作成情報を知っている者には、新たなラテン方陣の作成が、容易、かつ、正確にできる。

【図面の簡単な説明】

【図1】本発明作成装置の一実施の形態のブロック図である。

【図2】本発明により作成するラテン方陣の構成を示す図である。

【図3】本発明作成方法の一実施の形態を説明するフローチャートである。

【図4】本発明作成方法によるラテン方陣の作成手順の一例の具体的説明図である。

【図5】本発明作成方法によるラテン方陣の作成手順の他の例の具体的説明図である。

【図6】本発明により作成するラテン方陣の作成方向の説明図である。

【図7】ラテン方陣の各例の説明図である。

【図8】ラテン方陣の基本的構成説明図である。

【符号の説明】

1　演算部
2　ラテン方陣作成部
3　行位置設定用記憶部
4　列位置設定用記憶部
5　行位置比較用記憶部
6　列位置比較用記憶部
7　設定用記号記憶部
8　比較用記号記憶部
9　記号比較部

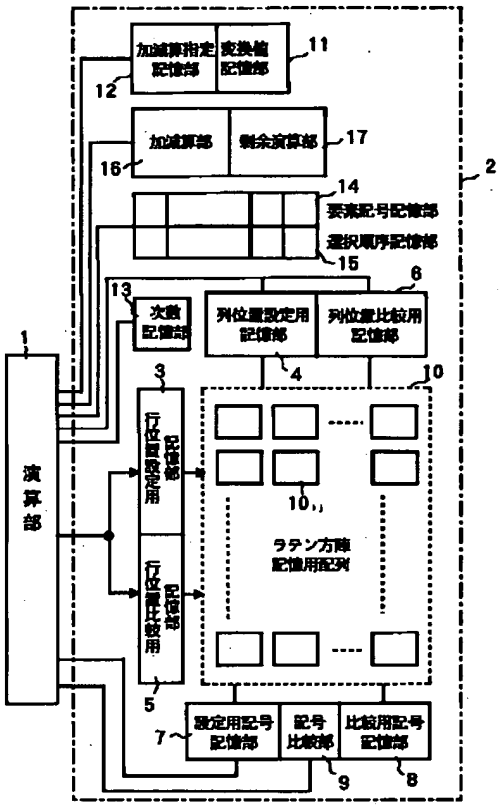
17

10　ラテン方陣記憶用配列
10I J　配列子（記憶素子）
11　変換値記憶部
12　加減算指定記憶部
13　次数記憶部

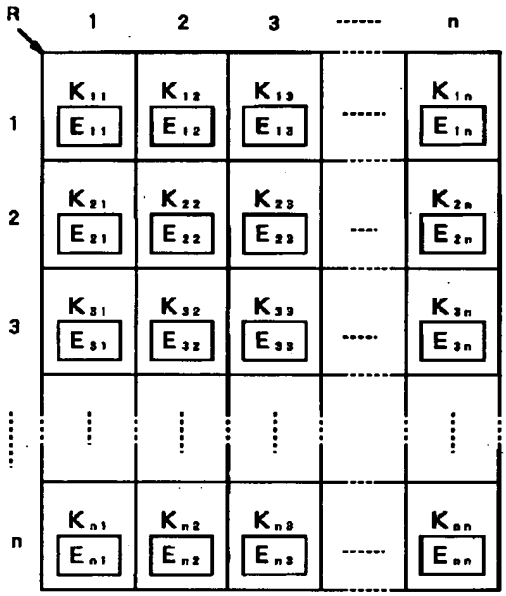
18

14　要素記号記憶部
15　選択順序記憶部
16　加減算部
17　剰余演算部
R　ラテン方陣

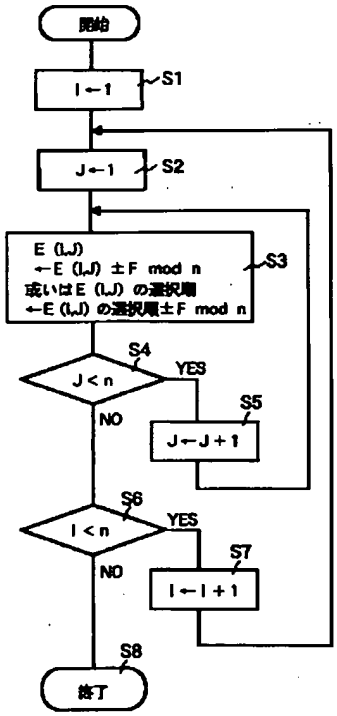
【図1】



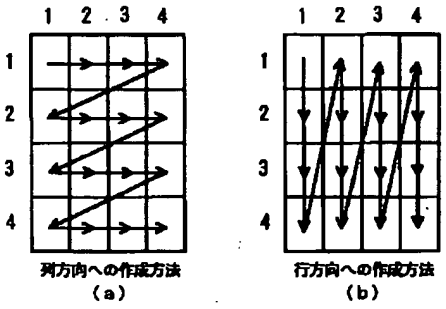
【図2】



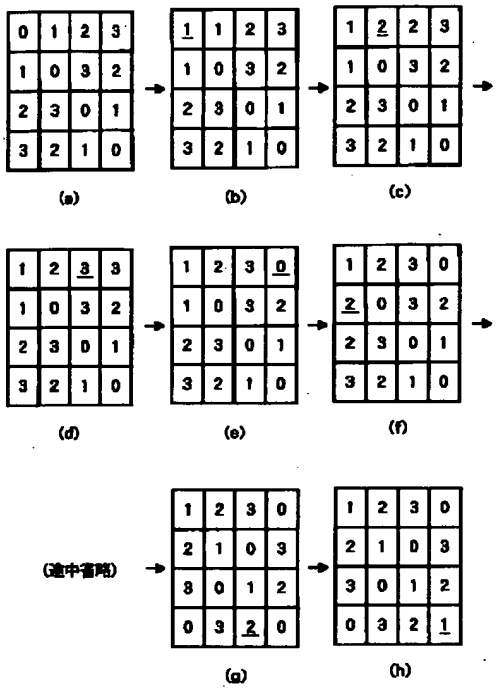
【図3】



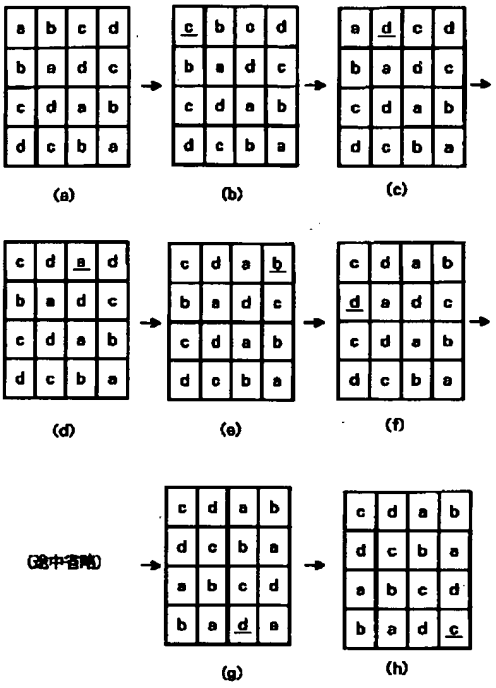
【図6】



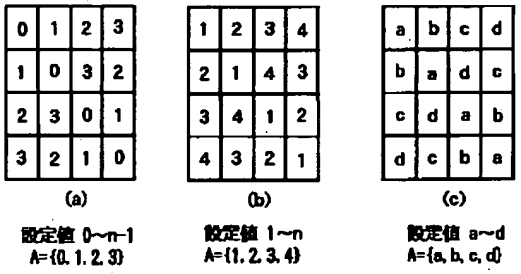
【図4】


(a)
(b)
(c)
(d)
(e)
(f)
(途中省略)
(g)
(h)

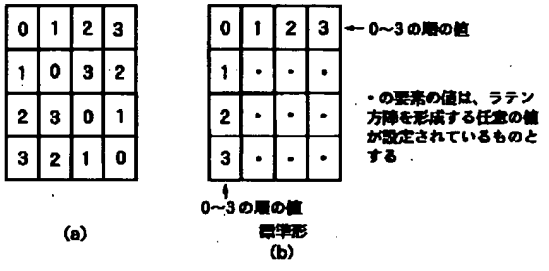
【図5】


(a)
(b)
(c)
(d)
(e)
(f)
(途中省略)
(g)
(h)

【図7】


(a)
設定値 0~n-1
A={0, 1, 2, 3}
(b)
設定値 1~n
A={1, 2, 3, 4}
(c)
設定値 a~d
A={a, b, c, d}

【図8】


(a)
0~3の順の値
0~3の順の値
標準形
(b)
・の要素の値は、ラテン方陣を形成する任意の値が設定されているものとする